DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA EVC GTS

Global Trusted Sign

Referência do Documento | DP03_GTS_V9

Índice

1. Referências	Regulamentação Europeia N.º 910/2017 CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.6.0; RFC 3161 – Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) ETSI EN 319 401 ETSI EN 419 421 ETSI EN 419 422 FIPS 140-2 Nivel 3
2. Documentos Associados	DP01_GTS Declaração de Práticas de Certificação da ROOT CA GTS DP06_GTS - Declaração de Divulgação de Princípios da EVC GTS
3. Lista de Distribuição	Grupos de confiança da GTS
4. Histórico do Documento	31-07-2017 | Versão 1 12-09-2017 | Versão 2 16-02-2018 | Versão 3 05-03-2018 | Versão 4 09-05-2018 | Versão 5 05-04-2019 | Versão 6 04-05-2020 | Versão 7 24-06-2020 | Versão 8 17-09-2020 | Versão 9
5. Classificação do Documento	D | Público

6. Registo da revisão

N.º da Versão	Elaborado	Aprovado	Motivo
	17-09-2020	17-09-2020	
9	AdmSeg	Grupo de Gestão	Atualização de registos de colaborador do Grupo de Confiança da GTS
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 17-09-2020 17:42:20	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 17-09-2020 17:45:15	

7. Âmbito

O presente documento especifica as políticas e os procedimentos que serão seguidos pela Global Trusted Sign, enquanto prestadora qualificada de serviços de confiança no âmbito do regulamento 910/2014 (adiante designada por GTS), no suporte à sua atividade de emissão de selos temporais qualificados da Entidade Certificadora de Validação Cronológica da Global Trusted Sign (adiante designada por EVC GTS).

7.1. Público-Alvo

O presente documento apresenta-se disponível publicamente e é destinado a todos os participantes que se relacionem, de alguma forma, com a EVC da GTS.

7.2. Estrutura do Documento

No âmbito da presente declaração de práticas assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique, recomenda-se o estudo prévio acerca dos referidos tópicos, permitindo assim uma melhor compreensão do presente documento.

De forma a facilitar a leitura e consequente análise deste documento com as práticas difundidas e recomendadas internacionalmente, optou-se por incluir todas a secções estabelecidas no índice da norma "ETSI EN 319 421 v1.1.1. Policy and Security Requirements for Trust Service Providers issuing Time-stamps", pelo que se não houver nada designado sobre o assunto, será incluída a expressão "nada a assinalar".

Os acrónimos e definições estão definidos no Anexo A do presente documento.

8. Enquadramento

O presente documento de Declaração de Práticas de Validação Cronológica, ou DPVC especifica os requisitos de segurança, políticas e práticas aplicáveis pelo prestador qualificado de serviços de confiança que emita selos temporais qualificados. As políticas e requisitos de segurança encontram-se definidos em termos de requisitos para a gestão do ciclo de vida dos selos temporais qualificados em conformidade com as políticas de certificados existentes.

A presente DPVC aplica-se respeita e implementa os standards seguintes:

- Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE
- ETSI EN 319 421 v1.1.1 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
- ETSI EN A319 422 v1.1.1 "Time-stamping protocol and time-stamp profiles"
- ETSI EN 319 401 v2.2.1: General policy requirements for Trusted Service Providers

- RFC 3161 – Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)

O presente documento é a Declaração de Práticas de Validação Cronológica da EVC GTS cujo OID associado é: 1.3.6.1.4.1.50302.1.1.1.3.1.0, enquanto que o OID de boas práticas associado à Política de Certificados de Validação Cronológica é 0.4.0.2023.1.1 (conforme definido pela ETSI EN 319 421) e o identificor único da Politica de Certificados de Validação Cronológica é o 1.3.6.1.4.1.50302.1.1.2.3.1.0.

Este documento é identificado pelos dados constantes na seguinte tabela:

Informação do Documento	
Nome do Documento	Declaração de Práticas de Certificação da EVC GTS
Versão do Documento	9.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.1.3.1.0
Data de Emissão	17 de setembro de 2020
Validade	17 de setembro de 2021
Localização	https://pki.globaltrustedsign.com/index.html

Nota: Atualizações regulares neste documento são realizadas sempre que se justifiquem.

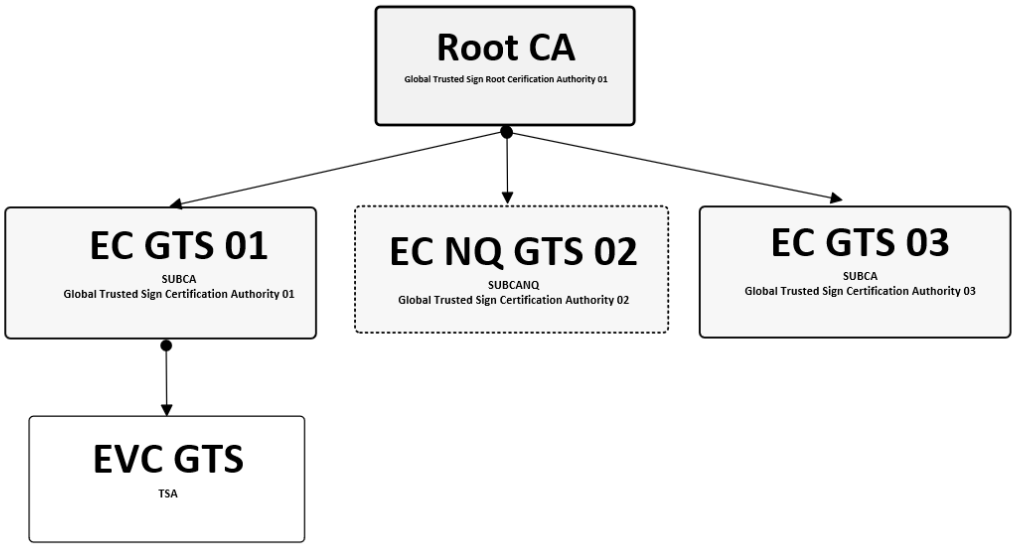
9. Participantes na Infraestrutura de Chave Pública

9.1. Entidades Certificadoras

A GTS, enquanto prestador qualificado de serviços de confiança, disponibiliza uma hierarquia de confiança credenciada pelo Gabinete Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), conforme previsto na legislação portuguesa e europeia.

É composta por um conjunto de equipamentos, aplicações, recursos humanos e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir assim a adequada gestão do ciclo de vida dos certificados descritos no presente documento.

A hierarquia de confiança da GTS é composta pela Entidade Certificadora Raiz da GTS (ROOT CA GTS), a Entidade Certificadora Não Qualificada da GTS (EC GTS), a Entidade Certificadora da GTS (EC GTS) e a Entidade Certificadora de Selos Temporais da GTS (EVC GTS). Estas entidades certificadoras estão descritas nos pontos 9.1.1, 9.1.2 e 9.1.3 do presente documento e encontram-se ilustradas de seguida:



Legenda:

1 – **Root CA GTS** - Entidade Certificadora Raiz da GTS
2 – **EC GTS 01** – Entidade Certificadora da GTS
3 – **EC NQ GTS 02** – Entidade Certificadora Não Qualificada da GTS
4 – **EVC GTS** – Entidade Certificadora de Validação Cronológica da GTS
5 – **EC GTS 03** – Entidade Certificadora da GTS

9.1.1. Entidade Certificadora Raiz da GTS (ROOT CA GTS)

A Root CA GTS é uma entidade certificadora credenciada pelo Gabinete Nacional de Segurança, de acordo com o Regulamento (UE) N.º 910/2014, estando deste modo habilitada, legalmente, a emitir certificados para Entidades Certificadoras Subordinadas.

O certificado da ROOT CA GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	7d 9f 44 7c b2 77 97 a8 59 57 bf 11 dd 8f 99 f5
Validade	01/07/2017 a 01/07/2037
Marca Digital	70 d1 2e f7 f5 90 18 87 47 88 42 c6 4e 05 ef 2c 0a 63 92 9d
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

9.1.2. Entidade Certificadora da GTS (EC GTS)

A Entidade Certificadora da GTS emite:

1. **Certificados qualificados para autenticação de sítios Web (SSL/TLS)**

   Os serviços de autenticação de sítios web fornecem meios que dão aos visitantes de um sítio web a garantia de que existe uma entidade genuína e legítima responsável pelo sítio. Estes serviços contribuem para a criação de segurança e confiança na realização de negócios *online*, pois os utilizadores têm confiança nos sítios web que tenham sido autenticados, pela garantia de autenticidade, titularidade e confidencialidade da informação transacionada.

   A prática de emissão de certificados qualificados para autenticação de sítios web da EC GTS está em conformidade com os requisitos do CA/Browser fórum disponíveis em http://www.cabforum.org:

   - Organization Validation: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.6.7
   - Extended Validation: Guidelines for the issuance and management of Extended Validation Certificates

Isso inclui a validação do domínio dos certificados requisitados (dono do domínio, domínio wild-card e CAA Records) conforme definido no CA/B Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.6.7 capítulo 3.2.2.

Em caso de inconsistência entre a DPC e os Requisitos do CA/B Forum, os Requisitos assumem precedência.

2. **Certificados para assinatura eletrónica qualificada**

   Os certificados para assinatura eletrónica qualificada permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo, bem como a integridade do documento.

3. **Certificados para selos eletrónicos**

   Os certificados para selos eletrónicos permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento.

O certificado da EC GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Certification Authority 001, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	5D F5 55 01 8C 89 45 56 59 8D CF D9 13 3B 87 AB
Validade	11/08/2017 a 11/08/2023
Marca Digital	2b 30 32 d4 9d 12 74 af 30 ab a3 ec 29 a6 a0 25 ae f6 dc bc
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Certification Authority 03, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	1e 0a 5a 4e b2 45 99 3c 5e b9 2f 31 48 db 0c f6
Validade	11/05/2020 a 11/05/2028
Marca Digital	60 2f 17 18 96 72 78 f5 88 4f 33 16 f2 65 9b c1 f3 cc b2 46
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

9.1.3. Entidade Certificadora de Selos Temporais da GTS (EVC GTS)

A EVC GTS é uma entidade certificadora de validação cronológica habilitada a emitir selos temporais qualificados.

A monitorização do serviço de emissão de selos temporais tem o objetivo de detetar qualquer desvio maior que os requisitos impostos pela norma ETSI EN 319 421 (conforme explicado no capítulo 9.4.3). Serão monitorizados todos os offsets entre as máquinas que suportam o serviço de emissão de selos temporais com o objetivo de gerar alarmística relevante que será usada para tomar iniciativas corretivas.

Esta EVC GTS tem a responsabilidade de operar uma ou mais TSU (*time-stamping unit*) para a criação e assinatura de selos temporais em nome da GTS, cada uma com a sua chave distinta de assinatura, cujo relógio utilizado para emitir selos temporais está sincronizado não só com o próprio relógio atómico da GTS, mas também, para efeitos de redundância, com mais duas fontes acreditadas conforme a norma ETSI EN 319 421.

O certificado da EVC GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Timestamping Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	04 bd 81 30 e4 ae 61 40 5a 99 43 db 7a 72 4f 47
Validade	02/03/2018 a 02/03/2023
Marca Digital	21 16 db 77 7e 72 fd 57 61 2a 24 27 8f d2 05 c8 bc fd a3 98
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

9.1.4. Entidade Certificadora Não Qualificada da GTS (ECNQ GTS)

A Entidade Certificadora da GTS emite:

Certificados avançados para assinatura pela Entidade Certificadora Não Qualificada da Global Trusted Sign, enquanto prestadora de serviços de confiança, que cumprem os requisitos definidos no Regulamento (UE) Nº 910/2014 (no que for aplicável), no ETSI EN 319 401, v2.1.1 e ETSI EN 319 411-1, v1.1.1.

O certificado da EC NQ GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign NQ Certification Authority 02, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	7e 88 a8 ed 54 02 9f c6 5c 96 00 8e 0a cf bd c1
Validade	23/03/2019 até 23/03/2025
Marca Digital	7e 55 0f f3 8f 70 2e eb 5d 8f f0 e2 02 75 78 3f be 83 57 38
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

9.2. Autoridade de Registo

A Autoridade de Registo (RA) é a entidade responsável pela análise e avaliação dos pedidos de serviços da GTS, nomeadamente à veracidade dos documentos e validação da identidade dos titulares dos certificados e pedidos. Esta RA tem o direito de aprovar ou rejeitar os pedidos após a devida validação. Adicionalmente a RA tem autoridade para aprovar a revogação de certificados.

As Autoridades de Registo da Global Trusted Sign estão em conformidade com os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas independentes, assim como Auditorias Internas realizadas Global Trusted Sign regularmente.

9.2.1. Autoridade de Registo Interna

No âmbito da Entidade de Certificação Global Trusted Sign, a autoridade de registo é executada pelos serviços internos da mesma, que têm responsabilidade de validação dos dados necessários, conforme explicitado nas Políticas especificas da Global Trusted Sign, para cada um dos serviços disponibilizados.

9.2.2. Autoridade de Registo Externa

A Global Trusted Sign, não dispõe de Autoridades de Registo Externas.

9.3. Subscritores e Titulares

Os subscritores são os titulares detentores de certificados que podem ser uma organização (pessoa coletiva) com vários utilizadores finais ou um utilizador final individual (pessoa singular).

9.4. Partes Confiantes

As partes confiantes são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de criação de um selo temporal.

9.5. Outros participantes

9.5.1. Entidade Supervisora

A Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras prestadoras de serviços de confiança qualificados.

No panorama nacional, essa função é desempenhada pelo Gabinete Nacional de Segurança (GNS). A Entidade Supervisora contribui para a confiança nos certificados qualificados, pelas competências que exerce sobre as EC que os emite. No âmbito das suas funções, a Entidade Supervisora exerce os seguintes papéis relativamente às Entidades Certificadoras:

- **Notificação de intenção:** procedimento de aprovação dos serviços de confiança prestados pelos prestadores de serviços qualificados, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, o hardware, software e os procedimentos de acesso e de operação;

- **Organismo de avaliação da conformidade:** enquanto organismo competente para realizar a avaliação da conformidade dos serviços de confiança prestados pelos prestadores de serviços qualificados;

- **Fiscalização:** Inspeções efetuadas para confirmar que tanto os prestadores qualificados de serviços de confiança como os serviços de confiança que prestam cumprem os requisitos estabelecidos pelo Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho.

9.5.2. Entidades Externas

A atividade dos prestadores de serviços que suportam a GTS no desempenho das suas funções enquanto prestadora qualificada de serviços de confiança é contratualizada de modo a garantir a atribuição formal das funções e responsabilidades de cada uma das partes.

9.5.3. Organismo de avaliação da conformidade

O Organismo de avaliação da conformidade (*Conformity Assessment Body* – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

9.5.4. Fonte da hora legal

Para efetuar a sincronização UTC necessária para a emissão de selos temporais é usado um relógio atómico com ligação GPS (Global Positioning System). Para satisfazer os requisitos de redundância impostos pela norma ETSI EN 319 412, foram configuradas mais duas fontes de tempo conforme imposto pela mesma norma. As fontes redundantes de tempo consideradas são:

- Royal Observatory of Belgium (ORB), Belgica, Bruxelas - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

10. Utilização do Selo Temporal

O objetivo dos selos temporais é garantir que um documento (ou ficheiro) existia num determinado momento no tempo. Esta garantia é obtida através da geração de um selo temporal qualificado emitido por uma entidade certificadora credenciada (como a EVC GTS) associado ao *hash* do documento ao qual será feita a aposição do selo temporal.

Deste modo, a associação de um selo temporal ao documento certifica não só a veracidade da hora e data do pedido, mas também a integridade e não repúdio do conteúdo.

Os selos temporais emitidos pela EVC GTS de acordo com esta DPC são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

10.1.1. Utilização adequada

Os selos temporais são emitidos a pedido dos subscritores, de acordo com a norma ETSI EN 319 421 e cumprem os requisitos impostos pela RFC 3161.

São também utilizados pelas Partes Confiantes para validação da associação da data/hora ao datum, devendo para tal:

- Verificar que o selo temporal foi corretamente assinado e que a chave privada utilizada para assina o selo temporal não foi comprometida até ao momento da verificação. Durante a validade do certificado da TSU, a validade da chave de assinatura pode ser verificada através da verificação do estado de revogação do certificado da TSU;
- Ter em consideração as limitações à utilização do selo temporal conforme definido nesta declaração de práticas e na política de certificados;
- Ter em consideração quaisquer outras precauções aplicáveis à utilização do selo temporal definida, por exemplo, em acordos.

Nota: Os requisitos e regras definidos neste documento aplicam-se a todos os selos temporais emitidos pela EVC GTS.

10.1.2. Utilização não autorizada

Os selos temporais não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente, ressalvada a exceção de poderem ser utilizados em outros contextos quando legalmente previstos na legislação aplicável.

11. Gestão das Políticas

A gestão da declaração de práticas de certificação da EVC GTS é da responsabilidade do grupo de Administração de Segurança da mesma.

Nome	**Grupo de Administração de Segurança da EVC GTS**
Morada	ACIN iCloud Solutions Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira Portugal
Correio Eletrónico	info@globaltrustedsign.com
Página Internet	https://www.globaltrustedsign.com
Telefone	707 451 451

A Declaração de Práticas de Certificação (DPC) deve ser aplicada internamente, bem como auditada internamente pelo grupo de trabalho Auditor de modo a garantir a sua conformidade. Esta auditoria deve resultar num relatório, que deve ser submetido ao Grupo de Gestão da EVC GTS, para aprovação.

11.1. Alterações às Políticas

Todos os documentos relacionados com a atividade da EVC GTS, incluindo o presente documento (DPC), e quaisquer alterações subsequentes, tornam-se efetivos após publicação no repositório.

A EVC GTS pode decidir em favor da eliminação ou emenda de um documento quando:

- Os seus conteúdos são considerados incompletos, imprecisos ou erróneos;
- Os seus conteúdos foram comprometidos.

O documento eliminado ou alvo de emenda é substituído por uma nova versão.

A validação da DPVC e consequentes correções ou atualizações são da responsabilidade do Grupo de Administração de Segurança e devem:

- Ser publicadas sob a forma de novas versões desta DPVC, substituindo qualquer DPVC anteriormente definida.
- Determinar, após alterações na DPC, se identificadores dos objetos (OID) devem ser alvos de alguma alteração.

O Grupo de Gestão é a entidade responsável pela aprovação e autorização de modificações destes documentos.

Todos os documentos relacionados com a atividade da EVC GTS, e quaisquer alterações subsequentes, permanecerão ativos até publicação de nova versão ou alteração.

11.2. Responsabilidades de Publicação e Repositório

A EVC GTS disponibiliza um repositório, em ambiente web, de informação relativa às práticas adotadas e o estado dos certificados emitidos, nomeadamente:

- **Entidade Certificadora Raiz da GTS (ROOT CA GTS)**
    - Certificado da ROOT CA GTS;
    - Lista de Revogação de Certificados (LRC) da ROOT CA GTS;
    - Declaração de Práticas de Certificação (DPC) da ROOT CA GTS;
    - Políticas de Certificados (PC) da ROOT CA GTS;
    - Outra informação relevante.

- **Entidades Certificadoras da GTS (EC GTS)**
  - Certificado da EC GTS;
  - Lista de Revogação de Certificados (LRC) da EC GTS;
  - Declaração de Práticas de Certificação (DPC) da EC GTS;
  - Políticas de Certificados da EC GTS;
  - Outra informação relevante.
- **Entidade Certificadora de Selos Temporais da GTS (EVC GTS)**
  - Certificado da EVC GTS;
  - Declaração de Práticas de Certificação (DPC) da EVC GTS;
  - Políticas de Certificados da EVC GTS;
  - Outra informação relevante.
- **Entidade Certificadora Não Qualificada da GTS (EC GTS)**
  - Certificado da EC NQ GTS;
  - Lista de Revogação de Certificados (LRC) da NQ EC GTS;
  - Declaração de Práticas de Certificação (DPC) da EC GTS;
  - Políticas de Certificados da EC NQ GTS;
  - Outra informação relevante.

O repositório das diversas entidades certificadoras pode ser acedido 24x7 em https://pki.globaltrustedsign.com/index.html. O repositório será atualizado sempre que haja uma alteração num dos documentos publicados.

A EVC GTS efetua as seguintes publicações, com a seguinte periocidade de publicação:

- O certificado da EVC GTS é publicado após a sua emissão;
- Novas versões ou alterações nas DPC e/ou respetivas Políticas de Certificados (PC), serão publicadas após a sua aprovação pelo Grupo de Gestão.

Foram implementados os seguintes mecanismos de controlo de acesso de segurança:

- Quaisquer alterações à informação publicada no repositório são efetuadas através de processos formais de gestão documental;

- A infraestrutura tecnológica que suporta o repositório e a sua publicação encontra-se em conformidade com as boas práticas de segurança da informação, incluindo os requisitos físicos bem como a gestão por uma equipa com as competências necessárias para a função;
- É garantido que o acesso à informação contida nos repositórios se efetua, apenas e só, em modo de leitura. Para tal, foram implementados mecanismos de segurança de forma a garantir que apenas pessoas autorizadas possam escrever ou modificar a informação contida nos repositórios.

12. Validação Cronológica

12.1. Emissão do selo temporal

O selo temporal é emitido de forma segura e de acordo com as recomendações da norma ETSI EN 319 422 com uma hora/data (timestamp) correta, possuindo os parâmetros seguintes:

- O identificador da política usada para a geração do selo temporal (0.4.0.2023.1.1)
- Um *timestamp*;
- Um *hash* criptográfico dos dados junto com o *timestamp*;
- Um serial number único;
- Um selo eletrónico gerado com a chave privada da EVC GTS, dedicada para esta função;
- Uma precisão mínima de 1 segundo em relação ao UTC, cuja sincronização de tempo da EVC GTS é feita com o próprio relógio atómico da GTS, ou com um dos dois servidores de tempo mencionados na alínea 9.5.4.

12.2. Sincronização do relógio

A GTS garante que o(s) relógio(s) que fornecem a hora/data (timestamp) incluída no selo temporal estão sincronizados uma precisão mínima de 1 segundo em relação ao UTC, respeitando as alíneas seguintes:

a) A calibração do relógio é mantida com uma precisão fiel à hora legal em vigor;

b) A sincronização do relógio é efetuada com recurso ao próprio relógio atómico da GTS ou com um dos dois servidores de tempo mencionados na alínea 9.5.4.

A correção do leap second é efetuada automaticamente pelo relógio atómico da GTS ou através da notificação automática vinda de uma das outras fontes redundantes (caso o relógio atómico não esta a funcionar). Os registros do processo de mudança temporal do leap second serão guardados e mantidos de forma automática junto com a hora exata desta alteração.

12.3. Processamento do pedido de selo temporal

O subscritor efetua o pedido de selo temporal, cujo processamento é executado de imediato pela EVC e de forma automática de acordo com os limites indicados neste documento.

Em caso de perda de sincronismo dos serviços de validação cronológica, a EVC GTS não emitirá selos temporais até que seja reposto o estado normal de operação.

Em caso de comprometimento ou suspeita de comprometimento dos serviços de validação cronológica, a EVC GTS não emitirá selos temporais até que a situação esteja normalizada e as devidas medidas corretivas tenham sido implementadas com sucesso.

13. Controlos de Segurança Física, de Gestão e Operacionais

13.1. Controlos de Segurança Física

A EVC GTS foi desenhada de forma a proporcionar um ambiente seguro capaz de proteger os sistemas que suportam a atividade da EVC GTS. As operações da GTS são realizadas numa sala numa zona de alta segurança, dentro de um edifício que garante a existência de diversos níveis de segurança acessíveis apenas às pessoas que dele necessitem para desempenho das suas funções de confiança.

A GTS garante ainda que as suas zonas de alta segurança possuem todo o conjunto de características previstas, bem como os mecanismos necessários por forma a garantir as condições de segurança, no que concerne a:

- Localização física e tipo de construção;
- Acesso físico ao local;
- Energia e ar condicionado;
- Exposição à água / inundações;
- Prevenção e proteção face a incidentes/desastres tais como incêndios, inundações e semelhantes;
- Eliminação de resíduos;
- Salvaguarda dos suportes de informação.

Os suportes de informação sensível deverão ser armazenados, de forma segura, em cofres e de acordo com o tipo de suporte e classificação da informação. O acesso a estas zonas deve ser restrito a pessoas devidamente autorizadas.

No final do seu ciclo de vida, documentos e materiais em papel que contenham informações críticas deverão ser eliminados através de métodos eficazes que não permitam a reconstrução dos mesmos.

Outros equipamentos de armazenamento (discos rígidos e afins) devem ser devidamente limpos, de modo a não seja possível recuperar alguma informação através de formatações seguras, ou destruição física dos equipamentos. No caso de periféricos criptográficos, estes devem ser destruídos segundo as instruções e recomendações dos respetivos fabricantes.

13.2. Controlos dos Processos

A atividade de emissão de selos temporais da GTS, enquanto entidade certificadora de certificados qualificados, exige o cumprimento de um conjunto de normas europeias.

Estas mesmas normas definem um conjunto de grupos de trabalho, com competências, atividades e regras distintas, que deve ser garantido pela GTS.

Na GTS todos os elementos (colaboradores, fornecedores ou consultores) que tenham acesso ou que controlem operações criptográficas ou de autenticação estão inseridos num determinado grupo de trabalho dependendo das suas funções.

13.2.1. Grupo de Trabalho da Administração de Segurança (AdmSeg)

Responsabilidades: Responsáveis globais sobre segurança dos sistemas, nomeadamente, pela gestão e implementação das regras e práticas de segurança no âmbito dos serviços prestados pela GTS.

Descrição de Tarefas:

- Definição da documentação associada às práticas de segurança da informação da GTS
- Definição dos procedimentos relacionados com a gestão das chaves criptográficas
- Garantia de que toda a documentação associada à GTS se encontra atualizada, adaptada à realidade e armazenada de forma segura de acordo com a sua classificação
- Gestão da implementação das práticas e políticas de segurança, incluindo o controlo de acessos lógico e físico
- Gestão dos riscos associados aos serviços prestados pela GTS
- Monitorização dos eventos de segurança e gestão da alarmística associada a estes
- Participação e resposta aos incidentes de segurança
- Guarda dos artefactos sob a sua custódia

13.2.2. Grupo de Trabalho da Administração de Sistemas (AdmSist)

Responsabilidades: Responsáveis pela instalação, configuração e manutenção dos sistemas, no entanto, com acesso controlado às configurações relacionadas com a segurança.

Descrição de Tarefas:

- Gestão do ambiente de produção
- Instalação, configuração e manutenção dos sistemas e rede tendo acesso controlado às configurações relacionadas com os componentes aplicacionais

- Gestão do desempenho dos sistemas que suportam a atividade da GTS, de modo a garantir que a infraestrutura esteja sempre disponível e operacional, previsão das necessidades futuras que decorrem da atividade da GTS e os seus custos
- Gestão dos incidentes e avarias de *hardware* e *software*
- Reposição do sistema através das cópias de segurança, quando necessário
- Execução e manutenção de documentação (procedimentos) pertinentes à execução das suas funções
- Guarda dos artefactos sob a sua custódia

13.2.3. Grupo de Trabalho de Operação de Sistemas (OpSist)

Responsabilidades: Responsáveis pela operação de rotina dos sistemas de confiança, estando autorizados a realizar as cópias de segurança e sua recuperação.

Descrição de Tarefas:

- Operação diária dos sistemas
- Realização de operações de rotina
- Realização de cópias de segurança
- Guarda dos artefactos sob a sua custódia

13.2.4. Grupo de Trabalho de Administração de Registo (AdmReg)

Responsabilidades: Responsáveis pela aprovação da emissão e revogação de certificados digitais (certificados de assinatura qualificada, selos eletrónicos, certificados para autenticação de sítios Web, e selos temporais).

Descrição de Tarefas:

- Emissão e revogação dos certificados
- Submissão dos Certificate Signing Request (CSR) para a execução dos processos de registo;
- Elaboração da videoconferência para validação da identidade dos titulares;
- Criação ou atualização das entidades requerentes de serviços de certificação;
- Validação da documentação a ser entregue pelo titular para emissão/revogação de certificados
- Validação da identidade dos titulares por videoconferência.
- Notificação dos titulares quando necessário
- Guarda dos artefactos sob a sua custódia

13.2.5. Grupo de Trabalho de Auditoria (Auditor)

Responsabilidades: Responsáveis pela análise interna da conformidade com as normas nacionais e europeias aplicáveis à atividade da GTS enquanto prestadora de serviços qualificados, estando autorizados a ver e monitorizar os arquivos de atividade dos sistemas de confiança.

Descrição de Tarefas:

- Registo e monitorização de todas as operações sensíveis do sistema
- Registo de todos os procedimentos passíveis de auditoria
- Verificação periódica da conformidade com os processos, políticas e procedimentos em vigor no âmbito da atividade de prestadora de serviços qualificados
- Guarda dos artefactos sob a sua custódia
- Apresentação de sugestões de melhoria

13.2.6. Grupo de Trabalho de Gestão (Gestão)

Responsabilidades: Responsáveis por assegurar os meios técnicos, financeiros e humanos para o correto funcionamento da GTS enquanto prestadora de serviços qualificados.

Descrição de Tarefas:

- Nomeação dos membros dos restantes Grupos de Trabalho
- Revisão e aprovação das Políticas e Declaração de Práticas da GTS
- Guarda dos artefactos sob a sua custódia

13.2.7. Número de pessoas exigidas por grupo

Cada grupo deverá ter pelo menos 2 pessoas de modo a garantir a redundância dos recursos.

13.2.8. Segregação de funções

A composição dos grupos de trabalho deve respeitar os princípios de privilégio mínimo e segregação de funções.

Deste modo, a tabela a seguir apresenta as incompatibilidades entre os diferentes grupos existentes na GTS, de modo a evitar quaisquer conflitos de interesse.

Grupo de Trabalho	Incompatível com				
	(a)	(b)	(c)	(d)	(e)
(a) Administração de Segurança		x	x	x	x
(b) Administração de Sistemas	x				x
(c) Administração de Registo	x				x
(d) Operação de Sistemas	x				x
(e) Auditoria	x	x	x	x	

13.3. Medidas de segurança de Pessoal

13.3.1. Requisitos relativos às qualificações, experiências, antecedentes e credenciação

Todos os membros que integrem um dos grupos de trabalho da GTS devem cumprir os seguintes requisitos:

- Apresentar provas da suficiente qualificação e experiência para o desempenho da respetiva função
- Garantir confidencialidade relativamente a informação sensível da GTS ou dados de identificação dos titulares
- Garantir que não desempenham funções que possam causar conflito com as suas responsabilidades nas atividades da GTS
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função
- Ter recebido a documentação necessária para o desempenho da respetiva função
- Ter recebido formação e treino adequado para o desempenho da respetiva função
- Ter sido nomeado formalmente para a função a desempenhar.

13.3.2. Procedimento de verificação de antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer um dos Grupos de Trabalho e inclui a verificação da identidade e do registo criminal, bem como das referências indicadas no curriculum vitae.

13.3.3. Requisitos de formação e treino

Os membros dos Grupos de Trabalho têm acesso a formação e treino adequado de modo a realizarem as suas tarefas de modo satisfatório e de forma competente, estando adicionalmente sujeitos a um plano que engloba os tópicos seguintes:

- Aspetos legais relativos à prestação de serviços de certificação
- Certificação digital e Infraestruturas de Chave Pública
- Conceitos gerais sobre segurança da informação
- Formação específica para o Grupo de Trabalho em causa
- Funcionamento do software e/ou hardware usado na GTS
- Política de Certificados e Declaração de Práticas de Certificação
- Procedimentos para a continuidade da atividade
- Recuperação face a desastres.

13.3.4. Frequência e requisitos para ações de reciclagem

Sempre que ocorra qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos existentes, deverá desencadear-se um processo de formação adequado para todos os Grupos de Trabalho. Devem ainda ser realizadas sessões formativas aos elementos das Entidades Certificadoras sempre que ocorram alterações às Políticas de Certificação ou na Declaração de Práticas de Validação Cronológica da GTS.

Tais factos devem ser tidos em linha de conta de modo a garantir o nível pretendido de conhecimentos para a execução satisfatória das responsabilidades que compete aos diferentes Grupos de Trabalho.

13.3.5. Frequência e sequência da rotação de funções

Nada a assinalar.

13.3.6. Sanções para ações não autorizadas

Todas as ações não autorizadas e que desrespeitem a Declaração de Práticas de Validação Cronológica da GTS e as Políticas de Certificados deverão ser alvo de medidas disciplinares adequadas, quer tenham sido realizadas de forma deliberada ou sejam ocasionadas por negligência.

Poderão ainda, de acordo com a gravidade da infração cometida, ser aplicadas sanções previstas na lei.

13.3.7. Requisitos para prestadores de serviços

O acesso à Zona de Alta Segurança por consultores ou prestadores de serviços independentes exige a supervisão contínua pelos membros dos grupos de trabalho, bem como o registo no livro de presenças existente para o efeito.

13.3.8. Documentação fornecida ao pessoal

Deverá ser disponibilizada aos membros dos Grupos de Trabalho a informação e documentação necessária relativamente às Políticas de Certificados, à Declaração de Práticas de Validação Cronológica da GTS, à documentação com a descrição das responsabilidades, obrigações e tarefas dependendo da função e ainda documentação técnica acerca do software e hardware utilizado na EVC GTS.

13.4. Procedimentos de auditoria de segurança

13.4.1. Tipo de eventos registados

Deverão ser registados todo o tipo de eventos significativos, capazes de ser auditáveis, em especial os seguintes:

- Cópias de segurança, restauro ou arquivamento de dados;
- Dispositivos físicos de segurança de entrada/saída dos vários níveis de segurança.
- Manutenções ao sistema;
- Modificações ou atualizações relativamente a software e hardware;
- Mudança de pessoal;

- Ligar e desligar aplicações ou sistemas que intervenham na atividade de certificação;
- Operações realizadas por membros dos Grupos de Trabalho;
- Tentativas, com ou sem sucesso, de acesso a recursos sensíveis da EVC GTS;
- Tentativas, com ou sem sucesso, de alteração dos parâmetros de segurança;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar contas do sistema;
- Tentativas, com ou sem sucesso, de início e fim de sessão;
- Tentativas, com ou sem sucesso, de operações relativas a pedido, emissão, renovação, modificação e revogação de chaves e certificados;
- Tentativas, com ou sem sucesso, de gerar, emitir ou atualizar LCR;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas, com ou sem sucesso, de acesso às Zonas de Alta Segurança da EVC GTS.

O registo dos eventos, efetuado quer por meios automáticos ou manuais, deverá conter, no mínimo, informações tais como a data e hora do evento, a categoria e descrição do mesmo, o número de série do evento, bem como a identificação do agente que o terá originado.

13.4.2. Frequência da auditoria de registos

A auditoria dos registos deverá ser realizada de forma regular, em especial na ocorrência de eventos que possam ser considerados suspeitos ou que possam comprometer, de alguma forma, a atividade em questão. Todos esses eventos deverão ficar registados num relatório sumário, passível de ser analisado, bem como as decisões e ações tomadas em resposta a estes.

13.4.3. Período de retenção dos registos de auditoria

Os registos de auditoria deverão ser mantidos nos sistemas por um período de pelo menos 1 mês após o seu processamento. Após esse período, deverão ser arquivados tal como definido na seção 14.5 do presente documento.

13.4.4. Proteção dos registos de auditoria

Os registos de auditoria devem encontrar-se protegidos contra as tentativas de acessos, alteração, manipulação ou destruição não-autorizadas.

Por norma, os registos eletrónicos devem estar protegidos com recurso a técnicas criptográficas de modo a que ninguém, à exceção das próprias aplicações de visualização de registos, com o controlo de acessos adequado, possa aceder aos mesmos.

Os registos manuais devem ser armazenados em locais que cumpram os requisitos definidos para o efeito, dentro de instalações seguras da EVC GTS. Este tipo de registos de auditoria é considerado informação sensível.

13.4.5. Procedimentos para a cópia de segurança dos registos

Devem ser realizadas cópias de segurança dos registos de auditoria de forma regular.

13.4.6. Sistema de recolha de registos (Interno / Externo)

Os registos são recolhidos e tratados centralmente.

13.4.7. Notificação de agentes causadores de eventos

Os eventos passíveis de serem auditáveis são registados nos sistemas internos da GTS, sendo estes armazenados de forma segura. Não está contemplada qualquer notificação ao agente causador do evento.

13.4.8. Avaliação de vulnerabilidades

Ainda que não ocorram alterações significativas no ambiente global da EVC GTS, deverão ainda assim ser efetuadas avaliações de vulnerabilidades, tendo em vista minimizar ou eliminar potenciais tentativas de quebras de segurança no sistema. O resultado das avaliações deve ser reportado aos responsáveis pela matéria, para que estes a possam rever e aprovar, caso se justifique, um plano de implementação e correção das vulnerabilidades detetadas., todos registos de eventos auditáveis devem ser regularmente analisados.

13.5. Arquivo de registos

13.5.1. Tipo de dados arquivados

A EC GTS irá arquivar, no mínimo, os seguintes tipos de dados:

- Os registos de auditoria especificados no ponto 13.4.1 do presente documento;
- As cópias de segurança dos sistemas que compõem a infraestrutura da EVC;
- Documentação relativa ao ciclo de vida dos certificados.
- Chaves para efeitos de confidencialidade (quando aplicável);
- Contratos estabelecidos entre a EC e outras entidades.

13.5.2. Período de retenção em arquivo

O tempo de retenção dos dados sujeitos a arquivo está definido de acordo com a legislação nacional, por um período nunca inferior a 7 anos.

13.5.3. Proteção dos arquivos

O arquivo encontra-se protegido de acordo com o que está igualmente previsto para a proteção dos registos de auditoria. Mais se acrescenta que o arquivo se encontra protegido de modo a que apenas os membros autorizados dos Grupos de Trabalho possam consultar e aceder ao mesmo.

13.5.4. Procedimentos para as cópias de segurança do arquivo

Segue igualmente o previsto no ponto 13.4.5, relativamente aos procedimentos para a cópia de segurança dos registos.

13.5.5. Requisitos para validação cronológica dos registos

Os registos contêm informações de data e hora (Timestamp) provenientes de uma fonte de tempo legalmente segura.

13.5.6. Sistema de recolha de dados de arquivo (Interno / Externo)

Os registos são recolhidos e tratados centralmente.

13.5.7. Procedimentos de recuperação e verificação de informação arquivada

Só os membros devidamente autorizados dos Grupos de Trabalho têm acesso aos arquivos para a verificação da integridade da informação, de modo a garantir que os mesmos se encontram em bom estado e que podem ser recuperados.

13.6. Recuperação em caso de desastre ou comprometimento

13.6.1. Procedimentos em caso de incidente ou comprometimento

Em caso de incidente de segurança grave ou comprometimento da EVC GTS, devem ser tomados os procedimentos seguintes:

- Notificação, sem demora indevida, mas sempre no prazo de 24 horas após ter tomado conhecimento do ocorrido, a entidade supervisora e, se necessário, outras entidades, como a entidade nacional competente em matéria de segurança da informação ou a autoridade responsável pela proteção de dados, de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados.

- Se a violação da segurança ou perda de integridade constatada for suscetível de prejudicar a pessoa singular ou coletiva a quem o serviço de confiança tiver sido prestado, será notificada também sem demora indevida a referida pessoa singular ou coletiva da violação da segurança ou da perda de integridade.

- Adicionalmente, e dependendo do tipo de incidente, a EVC afetada poderá ser desligada.

Se necessário, em particular se a violação da segurança ou a perda de integridade disserem respeito a dois ou mais Estados-Membros, a entidade supervisora notificada informa do facto as entidades supervisoras dos outros Estados-Membros em causa e a ENISA.

A entidade supervisora notificada informa o público ou exige que o prestador do serviço de confiança o faça, se considerar que a divulgação da violação da segurança ou perda de integridade é do interesse público.

Em caso de perda de sincronismo UTC do relógio da TSU, a TSU será reativada a partir do momento em que a normalidade seja reposta.

13.6.2. Comprometimento do Algoritmo

Se algum dos algoritmos, ou parâmetros associados, utilizados pela EVC GTS ou seus titulares se tornarem insuficientes para o fim a que se destinam, a EVC GTS deve:

- Informar todos os titulares e outras entidades com as quais a EVC GTS tenha acordos ou outra forma de relações estabelecidas. Adicionalmente, esta informação deve ser disponibilizada para outras entidades dependentes;
- Agendar a revogação de qualquer certificado afetado.

13.6.3. Corrupção dos recursos informáticos, do software e/ou dos dados

Caso os recursos de hardware, software e/ou dados tenham sido alterados ou exista a suspeita de que estes tenham sido corrompidos, deverá iniciar-se um processo de gestão de incidentes tendo em vista o restabelecimento das condições seguras com inclusão de novos componentes de eficácia credível.

A GTS suspenderá os seus serviços e notificará todas as Entidades envolvidas caso se verifique que esta situação tenha afetado os certificados emitidos, incluindo a notificação dos titulares dos mesmos.

13.6.4. Capacidade para continuidade da atividade

A GTS dispõe de um plano de continuidade da atividade, onde estão descritos todos os procedimentos a acionar em caso de desastre onde haja perda ou corrupção de dados, software e equipamentos.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade disponibilidade estão disponíveis no Local Alternativo e que os dados da EVC GTS necessários para retomar as operações são copiados e armazenados em locais seguros e adequados para permitir retomar devidamente as operações da EVC GTS em caso de incidentes/desastres.

As cópias de segurança de informações e software essenciais são realizadas regularmente. Devem ser fornecidas instalações de apoio adequadas para garantir que todas as informações e software essenciais possam ser recuperados após um desastre ou falha nos meios de comunicação (media). Os mecanismos de salvaguardas devem ser testados regularmente para garantir que respondem aos requisitos dos planos de continuidade do negócio.

13.6.5. Procedimentos em caso de extinção e cessação da EVC

A GTS deve em caso de cessação de atividades, atempadamente proceder às ações seguintes:

a) Informar a Entidade Supervisora (Gabinete Nacional de Segurança);

b) Informar todos os titulares dos certificados a partir de uma notificação explanatória com antecedência à cessação formal das atividades da EVC GTS;

c) Revogar todos os certificados;

d) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EVC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos;

e) Proceder à destruição definitiva de toda a informação classificada ou garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EVC GTS, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos. Esta decisão deverá ser tomada pela entidade Supervisora.

Em caso se procedam alterações do organismo/estrutura responsável de gestão da atividade da EVC GTS, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

14. Controlos de Segurança Técnicos

14.1. Gestão do ciclo de vida do par de chaves

A geração dos pares de chaves da EC GTS é processada de acordo com os requisitos e algoritmos definidos nesta declaração, através de um procedimento formal datado, realizado e assinado por elementos autorizados dos Grupos de Trabalho da Administração de Segurança e de Auditoria.

As chaves criptográficas geradas pela EVC GTS cumprem os impostos pelo Regulamento da União Europeia 910/2014, sendo assim armazenadas num "Qualified Signature/Seal Creation Device (QSCD)". O QSCD usado pela EVC GTS é um HSM credenciado a norma FIPS 140-2 Nível 3.

A EVC da GTS funciona em modo online.

No que respeita à dimensão das chaves, foram seguidas as recomendações da norma ETSI TS 119 312 – Electronic Signatures and Infrastructures – Cryptographic Suites. A geração das chaves da EVC GTS deverá ser feita de acordo com o estipulado no PKCS#1.

O algoritmo utilizado para assinatura do selo temporal é a função hash SHA-256 e o algoritmo de assinatura RSA, com a sha256RSA.

14.2. Proteção da chave privada e características do módulo criptográfico

A EVC GTS utiliza módulos criptográficos (HSM) para as operações que dizem respeito à geração, armazenamento e assinatura.

Os módulos criptográficos estão em conformidade com o Common Criteria v2.3, FIPS 140-2 nível 3 (para o módulo criptográfico da ROOT CA GTS).

A segurança do módulo criptográfico da EVC GTS é garantida durante o seu ciclo de vida, garantindo os seguintes:

- A instalação e ativação das chaves privadas no módulo criptográfico é efetuada por elementos de Grupos de Trabalho bem identificados (secção Controlos dos Processos e Medidas de Segurança de Pessoal);
- As chaves privadas de assinatura guardadas no módulo criptográfico são apagadas no final do seu ciclo de vida.

- O módulo criptográfico não foi adulterado durante o seu transporte;
- O módulo criptográfico não é adulterado enquanto permanece nas instalações seguras da GTS;
- O módulo criptográfico tem um funcionamento correto;

A EVC GTS efetua a retenção da sua chave privada e das chaves privadas de todos os seus clientes através de um HSM guardado em ambiente seguro.

As chaves privadas da EVC GTS:

- Têm pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original e são alvo de cópias de segurança
- São arquivadas internamente em ambientes seguros e por longos períodos de tempo.
- São geradas e armazenadas em HSM não sendo possível a transferência das mesmas para outros meios ou dispositivos.
- São armazenadas de forma cifrada em HSM.

A chave privada deverá ser ativada quando o sistema quando o sistema/aplicação da ROOT CA é ligado. Esta ativação só será efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação por quórum k em N onde k = 2. Isso é, é necessário k utilizadores em N para efetuar uma operação administrativa nos HSM (incluindo a ativação da chave privada). A chave privada permanecerá ativa até que o processo de desativação seja executado.

As várias chaves privadas da EC VGTS deverão ser destruídas sempre que deixem de ser necessárias. De uma forma geral, a destruição de chaves deve ser precedida sempre pela revogação do certificado, no caso de estar em vigor, ou caso tenha sido atingido o fim da sua data de validade. Nesse sentido, as chaves deverão ser apagadas/destruídas através de um método formal auditável, de modo a que não seja possível a sua posterior reconstrução. De igual forma, as respetivas cópias de segurança deverão também ser alvo de destruição.

14.3. Outros aspetos da gestão do par de chaves

Na GTS, o certificado digital é emitido pela EVC GTS de acordo com as práticas e políticas seguintes:

- Declaração de Práticas de Validação Cronológica da GTS;
- Política de Certificado de Validação Cronológica da EVC GTS.

14.4. Arquivo da chave pública

São armazenadas cópias das chaves públicas da EVC GTS mesmo após a expiração dos certificados correspondentes para verificação de assinaturas dos selos temporais durante o seu período de validade.

14.5. Período de validade do certificado e das chaves

A assinatura digital associada ao selo temporal tem uma validade diretamente proporcional ao certificado que a gerou. O certificado usado para as assinaturas dos selos temporais é o certificado da EVC GTS, cuja validade é de 5 anos.

14.6. Renovação de certificado com geração de novo par de chaves

No âmbito da GTS, a renovação dos certificados é feita através da geração de um novo par de chaves criptográficas de acordo com as práticas, políticas e procedimentos descritos na DPC ROOT CA GTS. Este processo é efetuado quando o certificado da EVC GTS atingir o termo de validade.

Nota: *Certificate re-key* é o processo de renovação em que é gerado um novo par de chaves e submetido o pedido para emissão de novo certificado que certifique a nova chave pública.

15. Medidas de segurança informática

15.1. Requisitos técnicos específicos

A EVC GTS tem um funcionamento online cujos pedidos de emissão de selos temporais são efetuados a partir de uma plataforma web disponível em https://www.globaltrustedsign.com. O acesso aos servidores da EVC GTS é restrito apenas a membros autorizados.

15.2. Avaliação / nível de segurança

Controlos contra acessos não autorizados:

- Duas Firewalls que dividem a infraestrutura física em duas zonas, uma Zona de Acesso Externo (ZAE) e uma Zona de Alta Segurança (ZAS);
- O uso de canais seguros no acesso às plataformas web públicas da GTS na ZAE nos respetivos portos/protocolos (HTTPS);
- O uso de canais seguros entre as Serviços e Servidores nas ZAS nos respetivos portos/protocolos (HTTPS);
- Todos os portos/protocolos não utilizados estão bloqueados pelas Firewalls.

Controlos contra modificações:

- Toda a comunicação entre componentes da infraestrutura da GTS é feita sobre o protocolo de HTTPS, protegendo deste modo a informação em trânsito.
- A plataforma web faz uso do protocolo HTTPS para proteção da informação em trânsito.
- A plataforma web só pode ser acedida pós autenticação dos utilizadores.

15.3. Ciclo de vida dos controlos de segurança

Todo o desenvolvimento, configuração e alteração do software/hardware associados à EVC são executadas e auditadas por membros autorizados da GTS.

A GTS possui mecanismos para controlar e monitorizar as configurações dos sistemas da EC GTS deste a sua primeira ativação até à eventual cessação de atividades, nomeadamente:

- Um sistema de monitorização na ZAS, que monitoriza entre outros aspetos, o espaço em disco dos servidores, a memória utilizada;
- Uma plataforma de ticketing para gestão de incidentes e agregação de eventos, inclusive eventos enviados pelo sistema de monitorização.

15.4. Verificação de selos temporais

A TSU da EVC GTS assina digitalmente os selos temporais dando uso a certificados digitais, cada um com uma validade de cinco anos. Durante esse período após a emissão do selo temporal, a validade do selo pode ser verificada, calculando o prazo entre a data de emissão e os 5 anos de validade.

16. Auditoria e Avaliação de Conformidades

A GTS irá efetuar auditorias e avaliações de conformidade regulares para assegurar a conformidade da Entidades Certificadoras constituintes da sua hierarquia de confiança de acordo com legislação nacional bem como com as normas internacionais aplicáveis.

Nota: A GTS, ou os seus representantes legais, podem delegar a realização destas auditorias, avaliações ou investigações a entidades externas de auditoria devidamente especializadas e acreditadas para o efeito.

16.1. Frequência ou motivo da auditoria

Na EC GTS, as auditorias de conformidade serão realizadas regularmente de acordo com a legislação aplicável por uma entidade externa registada e reconhecida para o efeito, tomando como base as normas existentes sendo os seus resultados comunicados à entidade supervisora.

16.2. Identidade e qualificações do Organismo de Avaliação da Conformidade

O Organismo de avaliação da conformidade (Conformity Assessment Body – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

16.3. Relação entre o Organismo de Avaliação da Conformidade e a Entidade de Validação Cronológica

O organismo de avaliação da conformidade e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

O Auditor e a parte auditada (Entidade Certificadora) não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares da EVC GTS.

16.4. Âmbito da auditoria

Uma auditoria de segurança é efetuada com base nos requisitos definidos na presente DPVC e em conformidade com a legislação nacional aplicável. Tem por objetivo determinar a conformidade dos serviços com as Políticas de Certificados e com a DPC definida. Deve também determinar a correta adequação em relação a diversos documentos, nomeadamente a políticas de segurança, segurança física, avaliação tecnológica, declarações de práticas de certificação e políticas de certificados em vigor, contratos e políticas de privacidade.

Pode ser efetuada de forma completa ou parcial, e pode incidir sobre qualquer tipo de documentos/processos.

16.5. Procedimentos após uma auditoria com irregularidades identificadas

Quando são detetadas irregularidades numa auditoria, a CAB deve proceder da seguinte forma:

a) Documentar todas as irregularidades encontradas durante a auditoria;

b) No final do processo de auditoria, reunir com os responsáveis da entidade submetida a auditoria e apresentar de forma sucinta o relatório de primeiras impressões (RPI);

c) Elaborar o relatório de auditoria de acordo com as regras e práticas estabelecidas pela Entidade Supervisora;

d) Submeter o relatório de auditoria à Entidade auditada;

e) A entidade submetida à auditoria deve enviar um relatório de correção de irregularidades (RCI) para a Entidade Supervisora, descrevendo as ações, metodologia e tempo necessário para a correção das irregularidades identificadas;

f) A Entidade Supervisora após a análise do relatório submetido, consoante o nível de gravidade/severidade das irregularidades, tomará uma das três opções seguintes:

   a. Aceitar os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;
   b. Permitir que a entidade continue em atividade por um período máximo de 90 dias para a correção das irregularidades;
   c. Revogação imediata das atividades.

16.6. Comunicação de resultados

Os resultados de todo o processo serão comunicados aos auditores responsáveis e à GTS.

17. Outras Situações e Assuntos Legais

Estabelecem-se outras situações, aspetos legais e de negócio que importa destacar:

- As taxas a ser cobradas para emissão e/ou reemissão de selos temporais, estão disponíveis no portal da Global Trusted Sign, ou são informadas mediante envio de proposta;
- Não serão cobradas taxas pela disponibilização dos certificados em repositório;
- O acesso a informação sobre o estado ou lista de revogação de certificados (LRC) é livre e gratuita, não se podendo aplicar qualquer taxa;
- Não estão previstos reembolsos aplicáveis à prestação de serviços de revogação de certificados.

17.1. Responsabilidade financeira

17.1.1. Seguro de cobertura

A GTS dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

17.1.2. Outros recursos

Nada a assinalar.

17.1.3. Seguro ou garantia de cobertura para utilizadores

A GTS dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

17.2. Confidencialidade da informação processada

O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular terá de ser expressamente autorizado pela própria.

Considera-se informação confidencial:

- As chaves privadas das Entidades Certificadoras;
- As chaves privadas dos titulares dos certificados;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal proporcionada à EC GTS durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;

- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Dados dos membros dos grupos de trabalho da EC GTS.

Considera-se informação de acesso público:

- Declarações de Práticas de Certificação;
- Políticas de Certificados;
- Listas de Revogação de Certificados (LRCs);
- Toda a informação classificada como "pública".

A ROOT CA GTS permite o acesso a informação não confidencial, sem prejuízo do que se venha a estabelecer nas DPC, no domínio dos controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

17.2.1. Responsabilidades de proteção da confidencialidade da informação

A EVC GTS garante a segurança de informação confidencial, evitando que esta possa ser comprometida por terceiros.

17.3. Privacidade dos dados pessoais

Informação privada é toda a informação fornecida pelo titular do selo temporal que não esteja publicamente disponível. Informação considerada não-privada é toda a informação tornada pública a partir do selo emitido e, como tal, não é considerada privada.

A responsabilidade de proteção da informação privada, assim como os procedimentos para notificação e consentimento para utilização da informação privada estão de acordo com a legislação portuguesa, nomeadamente com o regulamento geral de proteção de dados (regulamento 2016/679).

As práticas da EVC GTS garantem a proteção da confidencialidade e integridade dos dados de registo, especialmente quando transmitida entre a EVC GTS e os subscritores e titulares, bem como durante a comunicação entre os componentes distribuídos dos sistemas da EVC GTS.

No âmbito dos serviços prestados, é necessário manter evidências digitais por questões de conformidade com a legislação em vigor e aplicável à EVC GTS. Estas evidências são mantidas de modo a garantir a sua recolha, transmissão e armazenamento seguros.

17.4. Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a selos temporais emitidos pela EVC GTS, DPC, PC, bem como qualquer outro documento relacionado, são propriedade da GTS.

O titular conserva sempre o direito sobre as suas marcas, produtos ou nome comercial contidos nos selos.

17.5. Representações e garantias

É obrigação da EVC GTS cumprir as seguintes diretivas:

a) Colaborar com as auditorias dirigidas pela Entidade Supervisora;

b) Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais;

c) Declarar claramente todas as Práticas de Validação Cronológica num documento apropriado;

d) Em caso de cessação de atividades, comunicar o facto com uma antecedência mínima de três meses à Entidade Supervisora;

e) Emitir selos temporais de acordo com o RFC 3161 e que estejam conformes com os dados de pedido de selo temporal fornecidos pelo titular;

f) Empregar pessoal qualificado e experiente com conhecimentos necessários para a prestação de serviços de certificação;

g) Garantir a fiabilidade do processo de geração do selo temporal e da sua entrega ao subscritor;

h) Notificar, com a máxima brevidade possível, por meio de correio eletrónico, os titulares dos selos nos casos em que a EVC GTS proceda à revogação dos mesmos, indicando o motivo que originou a situação;

i) Operar em conformidade com as políticas, normas e legislação que sejam aplicáveis;

j) Proteger as chaves privadas da organização para assinatura dos selos;

k) Publicar a presente DPC e as Políticas aplicáveis no seu repositório, garantindo o acesso às versões atuais ou anteriores;

l) Realizar as atividades de acordo com a presente Declaração de Práticas;

m) Utilizar sistemas e produtos, protegidos contra alterações inesperadas e que garantam a segurança técnica e criptográfica dos processos de emissão de selos.

Os titulares dos selos temporais têm de obedecer às diretivas seguintes:

- Limitar e adequar a utilização dos certificados de acordo com a legislação vigente e com as utilizações previstas no presente documento;
- Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado o período de validade;

- Submeter às Entidades Certificadoras (ou de Registo) a informação que considerem exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;
- Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da EC GTS.

As partes confiantes dos selos temporais emitidos têm de obedecer às diretivas seguintes:

- Limitar a fiabilidade dos selos temporais às utilizações permitidas para os mesmos em conformidade com a legislação vigente e com o presente documento;
- Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
- Assumir a responsabilidade na correta verificação dos selos temporais;
- Assumir a responsabilidade na comprovação da validade, revogação dos certificados em que confia;
- Verificar que todos os parâmetros dos selos emitidos estão corretos com os dados fornecidos;
- Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
- Notificar qualquer acontecimento ou situação anómala relativa aos certificados, utilizando os meios que a EVC GTS publique no seu espaço Web.

17.5.1. Representação e garantias das Fontes Legais de Tempo

As fontes legais de tempo utilizadas pela EVC GTS têm de obedecer às diretivas seguintes:

a) Criar os meios e mecanismos necessários de modo a garantir o sincronismo entre o seu relógio e o relógio utilizado para a emissão de selos temporais;

b) Providenciar os meios necessários de forma a garantir o acesso de forma ininterrupto à hora fornecida;

c) Efetuar notificações na ocorrência de algum evento ou situação fora do expectável.

17.5.2. Renúncia de garantias

A EVC GTS recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPVC.

17.6. Limitações às obrigações

A GTS responde aos danos ou prejuízos causados aos titulares e partes confiantes decorrentes da sua atividade, conforme legislação aplicável.

A GTS não se responsabiliza por qualquer dano ou prejuízo decorrente das utilizações abusivas ou fora do âmbito do contrato estabelecido com os utilizadores e/ou partes confiantes.

A GTS não assume qualquer responsabilidade em caso falha dos serviços relacionada com causas de força maior, como desastres naturais, guerra ou outros similares.

17.7. Indemnizações

A GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável.

17.8. Termo e Cessação da Atividade

Esta DPVC entra em vigor desde o momento de sua publicação no repositório da EVC GTS e após aprovação, nos termos do presente documento.

Esta DPVC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão, nos termos do presente documento, ou pela renovação das chaves da ROOT CA GTS ou EVC GTS, momento em que, obrigatoriamente, se redigira uma nova versão.

Esta DPVC será substituída por uma nova versão, com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade.

Quando a DPVC ficar revogada será retirada do repositório público, garantindo-se, contudo, que será conservada durante o período definido no presente documento.

As obrigações e restrições que estabelece esta DPVC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da EVC GTS, nascidas sob a sua vigência, subsistirão após sua substituição ou revogação, por uma nova versão, em tudo o que não se oponha a esta.

17.9. Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar os mecanismos apropriados para a comunicação coletiva, onde se engloba o correio eletrónico assinado digitalmente, correio postal e formulários assinados, entre outros, recorrendo ao meio mais adequando em função da natureza de cada assunto.

17.10. Alterações

As alterações a esta DPC devem ser aprovadas pelo Grupo de Gestão. As alterações devem ser efetuadas através de documentos, contendo as novas alterações à DVPC.

No caso em que o Grupo de Gestão julgue que as mudanças à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes, que se efetuou uma mudança e que devem consultar a nova DPC no

repositório estabelecido. O mecanismo de comunicação será o sítio da internet https://www.globaltrustedsign.com.

Se a EC GTS determinar que a alteração ao identificador (OID) da DPVC ou política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem implicar uma mudança no identificador da política de certificados.

17.11. Reclamações e Disposições para Resolução de Conflitos

As reclamações devem ser endereçadas ao Grupo de Gestão da EVC GTS, através de carta registada.

Qualquer litígio decorrente da interpretação ou aplicação deste documento regem-se pela lei portuguesa. Para regular esses litígios, as partes elegem o foro judicial da Comarca de Funchal, com exclusão de qualquer outro.

Todas as reclamações entre os utilizadores e a EVC GTS poderão ser comunicadas à Entidade Supervisora com a finalidade da resolução de conflitos que possam na eventualidade surgir.

17.12. Legislação aplicável

A seguinte legislação é aplicável às entidades certificadoras prestadoras de serviços de confiança:

a) Regulamento (UE) N. o 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE

b) Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

17.12.1. Conformidade com a legislação em vigor

O presente documento (DPVC) é objeto de aplicação das leis que vigoram em território nacional, bem como das normas e legislações europeias.

17.13. Variadas Providências

As partes confiantes assumem, na sua totalidade, o conteúdo da última versão desta DPVC.

Em caso, de existirem uma ou mais estipulações do presente documento, que sejam ou tendam a ser inválidas, nulas, ou irreclamáveis em termos jurídicos, deverão ser consideradas como não efetivas. Estas determinações são válidas, apenas e só apenas nos casos em que tais estipulações não sejam consideradas essenciais. É da responsabilidade do Grupo de Gestão avaliar a essencialidade das mesmas.

As práticas adotadas pela EVC GTS garantem a independência dos membros dos grupos de confiança e da administração de topo, e a liberdade face a pressões comerciais, financeiras ou outras que possam influenciar a confiança nos serviços por eles prestados.

A EVC GTS disponibiliza certificados de teste para os atuais e potenciais utilizadores dos serviços a partir do site https://www.globaltrustedsign.com.

A EVC GTS garante as condições para que os seus serviços sejam utilizados por pessoas com deficiência, em conformidade com o regulamento europeu 910/2016.

17.14. Anexo A – Definições e Acrónimos

Acrónimos	
C	*Country*
CN	*Common Name*
DN	Nome Distinto *(Distinguished Name)*
DPVC	Declaração de Práticas de Validação Cronológica
DR	Decreto Regulamentar
EC	Entidade Certificadora
ER	Entidade de Registo
GNS	Gabinete Nacional de Segurança
GTS	*Global Trusted Sign*
HSM	Modulo Criptográfico em Hardware (*Hardware Secure Module*)
LRC	Lista de Revogação de Certificados
O	*Organization*
OU	*Organization Unit*
OID	Identificador de Objeto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	Infraestrutura de Chave Pública *(Public Key Infrastructure)*
SSL/TLS	*Secure Sockets Layer / Transport Layer Security*

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar
Assinatura Eletrónica Avançada	Assinatura eletrónica que obedeça aos requisitos: a) Esteja associada de modo único ao signatário b) Permita identificar o signatário c) Seja criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo, e d) Esteja ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados
Autenticação	Processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
Certificado de Assinatura Eletrónica	Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo
Certificado de Autenticação de Sítio Web	Atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido
Certificado de Selo Eletrónico	Atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome
Certificado Qualificado de Assinatura Eletrónica	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Autenticação de Sítios Web	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Selo Eletrónico	Certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento europeu 910/2014
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública

Definições	
Termo	**Definição**
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves
Credenciação	Ato pelo qual é reconhecido a um prestador de serviços que o solicite e que exerça a atividade de entidade certificadora em conformidade com os requisitos definidos no Regulamento europeu 910/2014
Criador de um Selo	Pessoa coletiva que cria um selo eletrónico
Dados de Identificação Pessoal	Conjunto de dados que permita determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa coletiva
Dados de Validação	Dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico
Dados para a Criação de um Selo Eletrónico	Conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico
Dados para a Criação de uma Assinatura Eletrónica	Conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica
Dispositivo de Criação de Assinaturas Eletrónicas	*Software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas
Dispositivo de Criação de Selos Eletrónicos	*Software* ou *hardware* configurados, utilizados para criar selos eletrónicos
Dispositivo Qualificado de Criação de Assinaturas Eletrónicas	Dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Dispositivo Qualificado de Criação de Selos Eletrónicos	Dispositivo para a criação de selos eletrónicos que satisfaça *mutatis mutandis* os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Documento Eletrónico	Qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade Certificadora	Entidade ou pessoa singular ou coletiva credenciada como prestador qualificado de serviços de confiança pela entidade supervisora
Entidade de Registo	Entidade que aprova os Nomes Distintos (DN) das entidades subordinadas e, mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras
Função Hash	Operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.

Definições	
Termo	**Definição**
Hash ou Impressão Digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais
HSM	Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro
Identificação Eletrónica	O processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva
Infraestrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas
Meio de Identificação Eletrónica	Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha
OID	Identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica
Organismo de Avaliação da Conformidade	Organismo definido que é acreditado nos termos do regulamento 910/2014 como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados
Organismo Público	Entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato
Parte Confiante	As partes confiantes ou destinatários são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao datum, ou seja, confiam na veracidade do selo temporal.
Política de Certificado	Conjunto de regras que indica a aplicabilidade do certificado a uma comunidade específica e/ou classe de aplicação com requisitos de segurança comuns

Definições	
Termo	**Definição**
Prestador de Serviços de Confiança	Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança
Prestador Qualificado de Serviços de Confiança	Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora
Produto	*Hardware* ou *software*, ou componentes pertinentes de hardware ou software, que se destinem a ser utilizados para a prestação de serviços de confiança
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos
Selo Eletrónico Avançado	Selo eletrónico que obedeça aos requisitos: a) Esteja associado de modo único ao seu criador b) Permita identificar o seu criador c) Seja criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico, e d) Esteja ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico
Selo Temporal Qualificado	Selo temporal que satisfaça os requisitos: a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável, b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada, e c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente
Selos Temporais	Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento

Definições	
Termo	**Definição**
Serviço de Confiança	Serviço eletrónico geralmente prestado mediante remuneração, que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços, ou b) Na criação, verificação e validação de certificados para a autenticação de sítios web, ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços
Serviço de Confiança Qualificado	Serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento europeu 910/2014
Serviço de Envio Registado Eletrónico	Serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada
Serviço Qualificado de Envio Registado Eletrónico	Serviço de envio registado eletrónico que satisfaça os requisitos: a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança b) Garantirem, com um elevado nível de confiança, a identificação do remetente c) Garantir a identificação do destinatário antes da entrega dos dados d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado
Signatário	Pessoa singular que cria uma assinatura eletrónica.
Sistema de Identificação Eletrónica	Sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas coletivas
Titular	Ver Signatário.
Utilizador	Pessoa singular ou coletiva que utiliza a identificação eletrónica ou o serviço de confiança
Validação	Processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico

Definições	
Termo	**Definição**
Validação Cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos